UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/927,999	08/10/2001	Wael Diab	CIS01-25(4997)	7356

7590 02/22/2005

David E. Huang, Esq.
CHAPIN & HUANG, L.L.C.
Westborough Office Park
1700 West Park Drive
Westborough, MA 01581

EXAMINER	
SCHUBERT, KEVIN R	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/927,999	DIAB ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09132001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-22 have been considered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4,6-13,15-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Walmsley, U.S. Patent No. 6,816,968.

As per claims 1,10,19, and 22, the applicant describes a method for verifying that a module is from an approved vendor comprising the following steps which are anticipated by Walmsley:

a) obtaining vendor data and a first magic code from a module (Col 24, lines 55-60);

b) generating a second magic code based on the vendor data (Col 24, lines 61-63);

c) outputting a magic code valid signal when the second magic code matches the first magic code, and a magic code invalid signal when the second magic code does not match the first magic code (Col 24, lines 65-67; Col 25, lines 1-5);

The applicant describes a method where a pluggable module is authenticated based on interaction with the system and particular cryptographic functions. The invention is designed for the authentication and use of modules that are from approved vendors so that the system does not experience problems related to failures from poor quality modules from untrusted vendors.

Walmsley describes a system which is used to authenticate modules which are installed on a system (Col 1, lines 33-45). One example Walmsley gives is that of printer toner cartridges. Since printer systems work best with printer cartridges from trusted vendors, Walmsley creates a system where a module, such as a printer cartridge, is authenticated in order "to prevent poorly manufactured substitute consumables from damaging the base system. For example, poorly filtered ink may clog print nozzles in an ink jet printer" (Col 1, lines 43-45). As one can see from the Specification and the Claims, Walmsley's invention is described according to an authentication protocol for validating the authenticity of an untrusted authentication chip (Col 24, lines 33-35), and this authentication chip can be on any type of module including a transceiver as described by applicant.

Regarding part a), the vendor data is labeled as a data message. The first magic code, or the encryption of the random number and the data message, is delivered with the data message from the untrusted chip being authenticated to the trusted chip.

Regarding part b), the second magic code is the encryption of the random number and the data message in the trusted authentication chip.

Regarding part c), the first and second magic codes are compared and a valid/invalid signal is generated accordingly.

Regarding claims 10,19, and 22, the claims introduce the limitations of a module and a controller. Both the trusted authentication chip and the untrusted authentication chip being authenticated are modules, which inherently include a controller for executing data read, compare, and output functions. The claims read appropriately if the module described and the controller coupled to the module pertain to the trusted authentication chip since it is the one which outputs the magic code valid signal. Regarding part b), the vendor data, or data message, and the first magic code, or encryption of the data message and the random number, are originally obtained from the untrusted authentication chip. However, since they are stored in memory when they are received by the authentication chip, the controller does obtain the vendor data and the first magic code from the memory of the trusted authentication chip in instances such as when it compares the first magic code with the second magic code to generate the valid/invalid signal.

As per claims 2,7,11, and 16 the applicant describes the method of claims 1,6,10, and 16, which are anticipated by Walmsley (see above), with the following additional limitations that are met by Walmsley:

a) reading the magic key from the memory of the computerized device (Col 24, lines 61-63);

b) forming the second magic code based on the magic key and the vendor data (Col 24, lines 61-63);

The applicant should note that both the trusted authentication chip, which generates the second magic code, and the untrusted authentication chip, which generates the first magic code, both have two secret keys stored in memory. The second secret key (magic key) is used to generate the first and second magic codes.

Regarding claims 11 and 16, the use of a processor in the authentication chips is described by Walmsley (Col 86, lines 21-30).

Regarding claims 7 and 16, the description of the vendor data as having the above characteristics is described in the rejection for claims 6 and 15 (see below).

As per claims 3 and 12, the applicant describes the method of claims 2 and 11, which are anticipated by Walmsley (see above), with the following additional limitation which is also met by Walmsley:

Performing a message-digest algorithm operation on the magic key and the vendor data (Col 38, lines 53-63; Fig 6);

Fig 6 illustrates an embodiment of the invention where the chip being authenticated sends the vendor data (M) and the first magic code (Sk2 [R | M]) to the trusted chip (63 of Fig 6). The applicant should note that the first magic code is a signature algorithm as described in Col 38, lines 53-63. A signature algorithm is a message-digest algorithm with encryption. A variety of hash, or digest, algorithms which can be used are described in the Background to the Invention by Walmsley and the Summary of the Invention (Col 25, lines 31-36).

As per claims 4 and 13, the applicant describes the method of claims 1 and 10, which are anticipated by Walmsley (see above), with the following additional limitation which is also anticipated by Walmsley:

Forming the second magic code based on the module serial number (Col 24, lines 61-63; Col 55, lines 3-6);

The second magic code is an encryption based on the random number and the data message (Col 24, lines 61-63). The data message (M) contains the serial number (Col 55, lines 3-6).

As per claims 6 and 15, the applicant describes the method of claims 1 and 10, which are anticipated by Walmsley (see above), with the following additional limitation which is also anticipated by Walmsley:

Forming the second magic code based on the vendor identification number, the character string representing the vendor name, and the module serial number (Col 24, lines 61-63; Col 55, lines 3-6);

The second magic code is an encryption based on the random number and the data message (Col 24, lines 61-63). The data message (M) is described as including a variety of identification data, including serial numbers and batch numbers (vendor ID numbers). Though a character string representing the vendor name is not explicitly described, it is inherently included in the description of the data message portion of the untrusted authentication chip which can contain a wide variety of identification factors (Col 28, lines 57-58; Col 55, lines 3-6).

As per claims 8,9,17, and 18, the applicant describes the method of claims 1 and 10, which are anticipated by Walmsley (see above), with the following additional limitation which is also anticipated by Walmsley:

a) reading the vendor data from the non-volatile memory of the small form factor pluggable component (Col 24, lines 56-64; Col 26, lines 36-43);

The vendor data is read in both the untrusted authentication chip, where the vendor data originates (Col 24, lines 56-60) and the trusted authentication chip, where the vendor data is stored once it is received (Col 24, lines 61-63). Though small form factor pluggable components are not specifically referenced, the system is described according to a general system between two authentication chips, or two modules. Since the system is described in general terms, the two authentication chips can be applicable to authentication chips of any variety of modules, including small form factor pluggable components or GBIC communication transceiver components.

As per claim 20, the applicant describes a small form factor pluggable module comprising the following limitations which are anticipated by Walmsley:

a) operating circuitry (Col 86, lines 33-34);

b) a memory, coupled to the operating circuitry, that stores vendor data including (i) an error-checking value and (ii) a non-error checking magic code which is generated by performing a magic code operation on at least a portion of the vendor data and a magic key (Col 51, lines 29-34; Col 24, lines 55-63; Col 34, lines 30-32);

The use of an error checking value is described in Col 51, lines 29-34. Both the first and second magic codes depend on the magic key and the data message, or vendor data. The first magic code is described in Col 24, lines 55-60. The second magic code is described in Col 24, lines 61-63.

As described in the rejection for claims 8,9,17, and 18, Walmsley describes an authentication protocol which is applicable to authentication chips related to any type of module, including small form factor pluggable modules.

As per claim 21, the applicant describes the module of claim 20, which is anticipated by Walmsley (see above), with a combination of claim 6 (vendor data description) and claim 3 (message-digest algorithm) which have both been rejected and described above.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walmsley.

As per claims 5 and 14, the applicant describes the method of claims 4 and 13, which are met by Walmsley (see above), with the following limitations which are also met by Walmsley:

a) obtaining a second serial number from a second module (Col 55, lines 4-17);

b) outputting a serial number valid signal when the module serial number of the vendor data does not match with the second serial number from the second module, and a serial number invalid signal when the serial number of the vendor data matches with the second serial number from the second module (Col 55, lines 4-17);

Walmsley describes all the limitations of claims 4 and 13. Walmsley also discloses the idea that each authentication chip should contain a different serial number (Col 55, lines 4-17) and there should be a method in place to thwart an attacker's chance of installing an untrusted module and a corresponding untrusted authentication chip. Furthermore, Walmsley discloses the idea of outputting a valid or invalid signal which authenticates or fails to authenticate an authentication chip and its corresponding module based on the data message (Col 25, lines 6-12).

Though the pieces of claims 5 and 14 are mentioned by Walmsley and described above, Walmsley fails to disclose the specific method of outputting a valid/invalid signal based on whether two authentication chips have matching serial numbers. Given that all the pieces are disclosed by Walmsley, it would have been obvious to one of ordinary skill in the art at the time the invention was filed to

incorporate the use of outputting a valid/invalid signal based on whether two authentication chips have matching serial numbers as an extra element of security in the system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

***